Amendments to the Specification:

Please replace the paragraph beginning on page 3, line 16, with the following amended paragraph:

Accordingly, in one aspect, the present invention provides a secure system for searching electronic data files stored in a data repository system. The system includes a communications environment that houses a first agent program for a depositor computer of an electronic data file in the data repository system and a second agent ~~pogram~~ program for a first user computer with access privileges to the electronic data file. A manifest is accessible to and maintained by the first agent program. The first user computer has a record of its access privileges to the electronic data file which is accessible to and maintained by the second agent program. When changes are made to the manifest affecting the first user computer's access privileges to the electronic data file, these changes are communicated from the first agent program to the second agent program so that the first user computer's record of its access privileges can be updated. The first agent program is also able to verify the first user computer's access privileges to the electronic data file before the electronic data file is released to the second agent program.

Please replace the paragraph beginning on page 5, line 7, with the following amended paragraph:

~~Figure 4, consisting of~~ Figures 4A and 4B, [[is]] contain a flow diagram illustrating the process of document retrieval according to the invention;

Please replace the paragraph beginning on page 5, line 29, and ending on page 6, line 6, with the following amended paragraph:

In such conventional systems, the document deposited by the document originator 100 is normally not encrypted [[to]] so that the business partner 106 will be able to review the document on demand. This is because there are problems associated with decrypting documents in the prior art. Document decryption requires access to the private key of the document originator 100. To give access to its private key, the document originator 100 must either make itself available online during all times that decryption might be requested in order to perform the decryption itself (the issue of system availability), or must set up a scheme in advance to make its private key available directly to the business partner 106 or through a trusted proxy (not shown).

Please replace the paragraph beginning on page 6, line 18, with the following amended paragraph:

Thus, in ~~convention~~ conventional systems where documents are deposited for a period of time and are not encrypted (Figure 1), the third party administrator of the repository service 104 must be trusted with maintaining the integrity of the document.

Please replace the paragraph beginning on page 11, line 20, with the following amended paragraph:

The encrypted document, the document originator's notarized signature, and the non-repudiation receipt are all stored in the application server's repository or the application database (block [[318]] 314). The non-repudiation receipt is sent to the vault of the document originator (block 316). the vault of the document originator checks the correctness of the non-repudiation receipt (block 318) by verifying the signature of the encrypted document. The document originator's vault also checks the currency of the time stamp in the notarized signature (block 320). The tolerance for the time stamp is application dependent. If either of these tests fail, an error message is returned to the AS vault (block 322) and logged in the system. If the receipt is correct and current, the application running the user's vault returns the non-repudiation receipt to the originating user (block 324) to be cached locally for future reference, in the event proof is required that the document has been stored in the repository.

Please replace the paragraph beginning on page 12, line 8, with the following amended paragraph:

Figure 4 is a Figures 4A and 4B contain a flow diagram illustrating the steps, according to the preferred embodiment of the invention, which must take place to permit a document to be retrieved by a requester who has been authorized under a type of manifest maintained by the document originator for each document called an access control list (ACL). As in Figure 3, the process steps have been divided between the three actors, user, application server and requester, on the basis that the

a6

personal vaults of each are notional secure extensions of their respective work spaces.

Please replace the paragraph beginning on page 20, line 25, with the following amended paragraph:

a7

Where ~~the~~ a complete data restore of the document database, ACLs, capability lists and corresponding tokens stored in the vaults is performed, users authorized to access a document before TIME1, can also access it after TIME2. This means that if a user was authorized before TIME1, but the authority was revoked after TIME1 but before TIME2, the user will have document access until the document owner performs a check of the ACL token. All users should therefore do an ACL and capability list check following a compete data restoration.